AFRL-RI-RS-TR-2014-271

DOMAIN NAME SERVER SECURITY (DNSSEC) PROTOCOL DEPLOYMENT

SHINKURO INC.

OCTOBER 2014

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the 88th ABW, Wright-Patterson AFB Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2014-271 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/ S /	**/ S /**
FRANK H. BORN Work Unit Manager	WARREN H. DEBANY, JR Technical Advisor, Information Exploitation and Operations Division Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* OCT 2014	**2. REPORT TYPE** FINAL TECHNICAL REPORT	**3. DATES COVERED** *(From - To)* NOV 2009 – JUN 2014

4. TITLE AND SUBTITLE DOMAIN NAME SERVER SECURITY (DNSSEC) PROTOCOL DEPLOYMENT	**5a. CONTRACT NUMBER** FA8750-10-C-0020
	5b. GRANT NUMBER N/A
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Stephen D. Crocker	**5d. PROJECT NUMBER** HS28
	5e. TASK NUMBER 00
	5f. WORK UNIT NUMBER 10

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Shinkuro, Inc. 5110 Edgemoor Lane Bethesda MD 20814	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Research Laboratory/RIGA 525 Brooks Road Rome NY 13441-4505	**10. SPONSOR/MONITOR'S ACRONYM(S)** AFRL/RI
	11. SPONSOR/MONITOR'S REPORT NUMBER AFRL-RI-RS-TR-2014-271

12. DISTRIBUTION AVAILABILITY STATEMENT

Approved for Public Release; Distribution Unlimited. PA# 88ABW-2014-4539
Date Cleared: 24 SEP 2014

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The DNSSEC Deployment Initiative was a 10-year effort to promote adoption of the DNS Security Extensions (DNSSEC), a method of cryptography securing domain name system (DNS) lookups. This report describes the latter five years of the initiative's work, which involved coordinating the activities of many private and public sector organizations to solve protocol, technical and deployment challenges related to DNSSEC. The initiative's work contributed to several major successes, including the signing of the DNS root zone and nearly all major top-level domains (TLDs). Remaining challenges include promoting wide adoption of DNSSEC signing and validation in the private sector, although progress was made in this area.

15. SUBJECT TERMS

DNS, DNSSEC, TLD, ccTLD, Internet Security

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** **FRANK H. BORN**
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	31	**19b. TELEPHONE NUMBER (*Include area code*)** **N/A**

Table of Contents

1. Summary ... 1
2. Introduction ... 1
3. Methods, Assumptions and Procedures ... 4
   3.1. DNSSEC Status at Start of Contract ... 4
      3.1.1. Protocol Specification ... 4
      3.1.2. Implementations ... 4
      3.1.3. Signing Status ... 4
      3.1.4. Validation Status ... 4
      3.1.5. Operating System Status ... 4
      3.1.6. Perceived Image ... 4
      3.1.7. Main Challenges ... 5
4. Results and Discussion ... 5
   4.1. DNSSEC Status at End of Contract ... 5
      4.1.1. Protocol Specification ... 5
      4.1.2. Implementations ... 5
      4.1.3. Stub Resolvers ... 5
      4.1.4. Signing Status ... 6
      4.1.5. Validation Status ... 6
      4.1.6. Operating System Status ... 6
      4.1.7. Perceived Image ... 6
      4.1.8. Current Challenges ... 6
   4.2. DNSSEC Deployment Initiative ... 7
      4.2.1. Communications and Coordination ... 7
      4.2.2. SOHO/Last-Mile Issues ... 8
      4.2.3. Timing Model ... 9
      4.2.4. Algorithm Signaling ... 12
      4.2.5. History of TLD DNSSEC Adoption ... 13
      4.2.6. Tracking and Mapping DNSSEC Adoption ... 14
      4.2.7. Users Guide ... 15
5. Conclusions ... 16

Appendix A: DNSSEC Presentations and Transcripts ... 17

List of Symbols, Abbreviations, and Acronyms ... 30

1. SUMMARY

The DNSSEC Deployment Initiative was a 10-year effort to promote adoption of the DNS Security Extensions (DNSSEC), a method of cryptographically securing domain name system (DNS) lookups. This paper describes the latter five years of the Initiative's work, which involved coordinating the activities of many private- and public-sector organizations to solve protocol, technical and deployment challenges related to DNSSEC from 2009–2014.

The Initiative's work contributed to several major successes, including the signing of the DNS root zone and nearly all major top-level domains (TLDs). Remaining challenges include promoting wide adoption of DNSSEC signing and validation in the private sector, although progress was made in this area as well.

2. INTRODUCTION

This is the final report for the Shinkuro, Inc. portion of the DNSSEC Deployment Initiative. The Initiative covered the period 2004–2014, funded under two separate contracts. This report covers the second contract, from 2009–2014.

The stated goal of the Initiative was to foster the deployment of DNSSEC throughout the entire DNS and for every query to be checked. While those goals remain in the future, significant progress was made during this period. The most visible progress was in the signing of the TLDs.

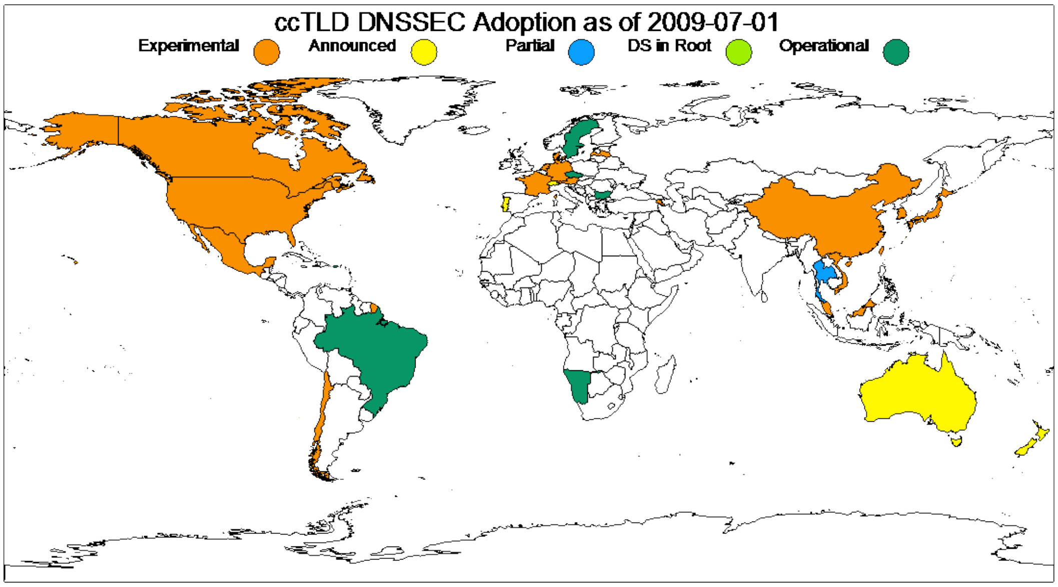
Table 1 shows the number of top-level domains in each of five categories that had a Delegation Signer (DS) record in the root zone in mid-2009, the number signed via a DS record by mid-2014, and the totals in each category. Country-code TLD (ccTLD) and generic TLD (gTLD) indicate the type of domain, while "Classic" means the TLD is in Latin letters. "IDN" stands for Internationalized Domain Name, i.e. the TLD is in some other script, such as Cyrillic, Chinese or Arabic. "Regional" consists of just .SU and .EU, for the old Soviet Union and the European Union. These operate under country-code rules but cover more than one country.

Table 1. TLDs with DS in the Root in Mid-2009 vs. Mid-2014

	Signed as of 1 July 2009	Signed as of 1 June 2014	Total TLDs as of 1 June 2014
Classic gTLD	2	280	300
Classic ccTLD	8	94	247
IDN gTLD	0	26	28
IDN ccTLD	0	10	39
Regional	0	2	2
Total	10	412	616

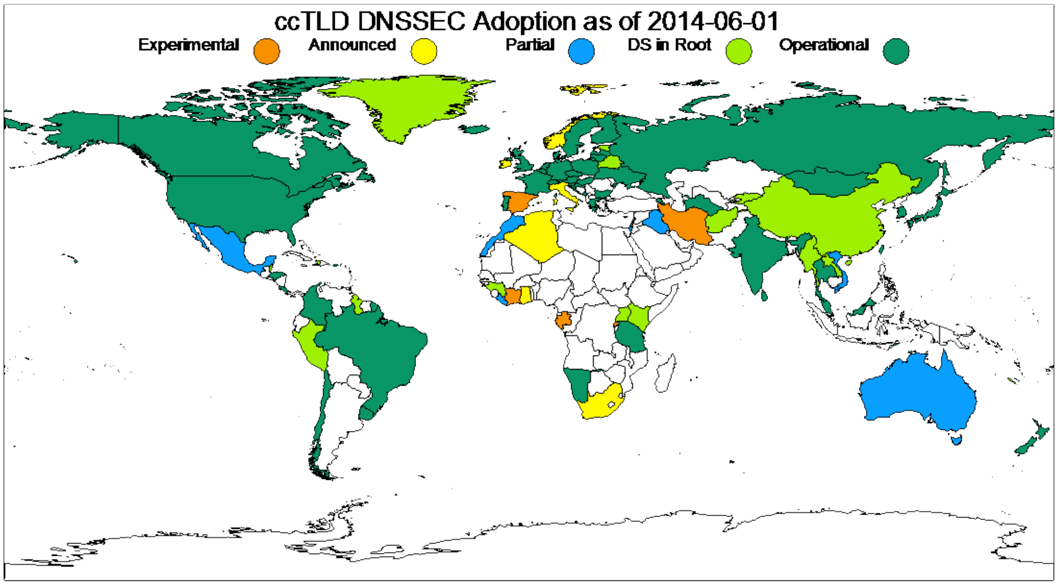
Maps showing the progress in the Classic ccTLD category from 2009–2014 are in Figures 1 and 2, and a more detailed discussion of the methodology underpinning them appears in Section 4.6.

Section 2 compares the status of DNSSEC deployment at the time of the contract's start in July 2009 and its end in June 2014, while subsequent sections cover specific actions we, DHS and other Initiative partners took to further deployment.



Experimental – Internal experimentation announced or observed (19):	AM AT CA CL CN DE DK FR JP KR LV MX MY NL RE TO TW US VN
Announced – Public commitment to deploy (6):	AU CH LI NZ PT SG
Partial – Zone is signed but not in operation (no DS in root) (1):	TH
Operational – Accepting signed delegations and DS in root (6):	BG BR CZ NA PR SE

Figure 1. DNSSEC Deployment Among the Classic ccTLDs in Mid-2009



Experimental – Internal experimentation announced or observed (6):	CI ES GA IR RW TO
Announced – Public commitment to deploy (7):	DZ GH IE IT NO SG ZA
Partial – Zone is signed but not in operation (no DS in root) (10):	AU HK IL IQ LR MA MS MX VC VN
DS in Root – Zone is signed and its DS has been published (29):	AD AF AG AW BY BZ CC CN EE FO GI GL GN GY HT KE KG KI LA LB LC MM NC NU PE PW SJ TV UG
Operational – Accepting signed delegations and DS in root (65):	AC AM AT BE BG BR CA CH CL CO CR CX CZ DE DK FI FR GR GS HN HR HU IN IO IS JP KR LI LK LT LU LV ME MN MU MY NA NF NL NZ PL PM PR PT RE RU SB SC SE SH SI SX TF TH TL TM TT TW TZ UA UK US UY WF YT

Figure 2. DNSSEC Deployment Among the Classic ccTLDs in Mid-2014

3. METHODS, ASSUMPTIONS AND PROCEDURES

The following paragraphs discuss the state of DNSSEC work at the time of Shinkuro's submission of its proposal in July 2009 (i.e. the assumptions under which Shinkuro's work was proposed) as well as the methods and procedures under which such work might take place.

3.1. DNSSEC Status at Start of Contract

3.1.1. Protocol Specification

Work was winding down on Next Secure 3 (NSEC3); the last major component was finished in 2007 and implementations had started to appear, but bugs and corner cases were being worked out both in code and in specifications. A document listing the errata on various DNSSEC RFCs had just appeared.

3.1.2. Implementations

At this time three implementations of DNSSEC had been released—BIND-9, Unbound/NSD and Nominum. Other organizations had done their own implementations in-house. Tools were limited but were starting to appear. Meanwhile, the U.S. government had mandated that DNSSEC be used by all .gov domains, which began to attract some vendors; but more importantly, were learning lessons on how to operate DNSSEC.

3.1.3. Signing Status

Only 10 TLDs out of 230, were signed at this point (.bg, .br, .cz, .na, .pr, .pt, .se, .th, museum, .org), although a small number of lower-level domains were signed around the world. The biggest issue was how to bootstrap trust anchors, with the main question being: Should that be handled by signing the root or via online trust anchor repositories (TARs)? TAR proponents argued that they would be needed as the root would never be signed and too few TLDs would ever sign their zones, while TAR opponents argued that they were inherently unsafe due to operational factors such as their acceptance policy for new trust anchors, how a domain could modify a trust anchor in a TAR, and how a domain could discover it was listed in a particular TAR.

3.1.4. Validation Status

Validation was difficult to perform due to the difficulties in getting and maintaining trust anchors, since all trust anchors were for islands of trust.

3.1.5. Operating System Status

No operating system distribution was distributing DNSSEC-enabled validators, but a number of Linux/BSD operating systems were shipping DNSSEC-capable software in their base distributions, allowing people to turn on DNSSEC if they so chose. There were also packages available that performed the seemingly magical task of configuring BIND to do DNSSEC signing and validation.

3.1.6. Perceived Image

The most common remarks about DNSSEC were "What is that?" and "Why bother?" followed by "That's a nice, complicated technology, but who needs it?” In third place: "Yes, this is needed and it will enable a number of new capabilities."

3.1.7. Main Challenges

The main challenge at this time was to convince the world that the root would be signed and a large number of TLDs would follow, thus enabling regular, non-TLD domains to be signed and validated to the root. There was also a fair amount of confusion regarding differences between the two negative answer records and debate about which was better: Was NSEC3 a replacement for NSEC, or was it an alternative? Getting outsourcers of DNS services and Web functions to start thinking about including DNSSEC capabilities was an uphill battle as they saw no need for it, only the difficulties and costs.

4. RESULTS AND DISCUSSION

The following sections discuss the state of DNSSEC adoption at the end of this contract, at the beginning of June, 2014.

4.1. DNSSEC Status at End of Contract

4.1.1. Protocol Specification

Work on the protocol specification has concluded and the core protocol can now be considered complete. The last major protocol development was the addition of NSEC3 (hashed denial of existence), and that was completed in 2007 after a number of interoperability workshops. Since then the only changes have been clarifications and fixes that were discovered during early-adopter deployments, and this work was itself completed in 2012. The deployment experience has shown that a number of operational aspects of the DNS can be automated when DNSSEC is in place, most of which relate to moving information from the child to the parent DNS operator via in-band mechanisms. While DNSSEC is a stable protocol it will need regular maintenance regarding the use of cryptography and hash algorithms, which is a direct consequence of advances in cryptography and improvements in computing power.

4.1.2. Implementations

By now all major implementations of authoritative DNS servers provide support for DNSSEC. DNSSEC was a major reason for the development of three new implementations (NSD, KNOT and Yadifa). There are a number of special DNS servers for various organizations that have not yet added DNSSEC capabilities; most of these are used by content distribution networks (CDNs) but a number have started creating special DNSSEC-supporting systems for their paying customers.

On the resolver side, many of the available recursive resolvers support DNSSEC or have plans to do so, including BIND, Unbound, Microsoft DNS and Nominum Vantio. Most recently, DNSMASQ added DNSSEC resolver support. There are few if any actively maintained DNS resolvers that do not support DNSSEC or at least have DNSSEC support in their development roadmap. There are also a new class of open public resolvers designed to be used by anyone, and some are used by large numbers of users; the largest, Google DNS, does full validation on all requests.

4.1.3. Stub Resolvers

There are some attempts to place DNS validation on end systems, and this works well for devices that stay on the same network all the time. For mobile devices, end-system validation is much more difficult due to the state of their networks, many of which do not allow fragmented

User Datagram Protocol (UDP); others capture all DNS traffic and route it through a limited-functionality middle box. Some tools have emerged to address this challenge, including DNSTrigger, an NLnet Labs project designed to maximize the chance for a device to validate. Other tools have been created to allow users to measure whether validation can take place. These developments are important because if edge devices can validate, they can then operate more safely anywhere in the world.

4.1.4. Signing Status

The major hurdle and unknown when this project began was the question of whether the root and large TLDs would be signed. The root was signed in June 2010, many of the bigger TLDs are signed (e.g. .com, .net, .org), and many countries' ccTLDs are signed (starting with .se and followed by many others since then). As of June 1, 2014 there were 603 delegations in the root zone and 418 TLDs signed; 408 of them have DS in the root and thus can be validated. The other 10 are in various stages of DNSSEC deployment. Significantly, all new TLDs are now required to have DNSSEC signing from day one.

The U.S. government's mandate to have all .gov domains DNSSEC-signed was instrumental in getting DNSSEC added to tools and DNS software. Although there were a number of operational events that caused outages during this process, this was to be expected as this was new code and not all corner cases were debugged before release. Over the last few years the number of these events has decreased even though the number of domains signed keeps increasing. In addition, the failures were not exclusively caused by software, but also by hardware failures as well as a number of operational failures or misunderstandings of the properties of the DNS and DNSSEC.

4.1.5. Validation Status

The hardest part of deploying DNSSEC has been to get people to start validating since many operators are worried about validation failures causing important domains to be unreachable. At this point, a declining number of reports of configuration errors and manual mistakes that cause DNS-validation failures indicates that there is hope for improvement.

A number of attempts have been made to create methods for measuring the current state of validation in the wild, with the best being to use advertisements in YouTube to look up names. Based on this measurement, over 12 percent of all users in the world are using DNSSEC-validating resolvers.

4.1.6. Operating System Status

Most operating systems ship with DNSSEC-capable software, leaving it up to the user to turn the validation on. However, Fedora-21 will be released this year and will be the first OS distribution to have DNSSEC validation turned on by default.

4.1.7. Perceived Image

There are still some lingering negative perceptions of DNSSEC, mainly among operators and CDNs, although DNS-based Authentication of Named Entities (DANE) is turning into a good attractor or driving force for DNSSEC adoption.

4.1.8. Current Challenges

DANE is an attempt to place information in the DNS that can be used to authenticate or create encrypted communication. This technology requires DNSSEC and is gaining traction as it allows better binding of keying information via the DNS than can be done by certificates. A number of protocols such as transport-layer security (TLS, i.e. HTTPS) and Simple Mail Transfer Protocol (SMTP) are in the process of adding DANE support, and work is being done to address the difficult problem of discovering an email recipient's key, and to enable Secure/Mutipurpose Internet Mail Extensions (S/MIME) and OpenPGP keys to be published in the DNS. Getting DANE deployed soon and quickly will increase DNSSEC use, as this is an operationally better and cheaper way to distribute keying information than the current public-key infrastructure (PKI) allows.

In addition, it will take work to convince CDNs and other operators with highly time-critical business operations to deploy DNSSEC, as well as to persuade financial institutions to adopt it.

4.2. DNSSEC Deployment Initiative

In this section we describe the details of various portions of the overall effort.

4.2.1. Communications and Coordination

Shinkuro was the Co-Chair of the DNSSEC Deployment Working Group, which included regular conference calls, mailing list contributions, and DNSSEC workshops at appropriate regional and international meetings.

Two to three major workshops were organized and conducted in conjunction with the regularly scheduled Internet Corporation for Assigned Names and Numbers (ICANN) meetings each year. Attendance varied between 50–100 people at each meeting. The DNSSEC workshops given during the period of the contract include:

- ICANN Meeting, Nairobi, Kenya, March 2010
- ICANN Meeting, Brussels, Belgium, June 2010
- ICANN Meeting, Cartagena, Uruguay, December 2010
- ICANN Meeting, San Francisco, California, March 2011
- ICANN Meeting, Singapore, Singapore, June 2011
- ICANN Meeting, Dakar, Senegal, October 2011
- ICANN Meeting, San Jose, Costa Rica, March 2012
- ICANN Regional Meeting, Prague, Czech Republic, June 2012
- ICANN Meeting, Toronto, Canada October 2012
- ICANN Meeting, Beijing, PRC, April 2013
- ICANN Meeting, Durban, South Africa, July 2013
- ICANN Meeting, Buenos Aires, Argentina, November 2013
- ICANN Meeting, Singapore, March 2014

A guide to the location of the presentations and supporting materials may be found in Appendix A: DNSSEC Presentations and Transcripts.

In addition, we created a DNSSEC Roadmap in 2013 that described progress toward the Deployment Initiative's ultimate goal—for all zones to be signed and all queries to be checked. The Roadmap detailed how the Initiative and DHS could be most effective in pushing DNSSEC adoption by enterprises toward a future tipping point, and how to increase validation by Internet

Service Providers (ISPs) and end users. The full Roadmap is available at http://www.shinkuro.com/FA8750-10-C-0020/Publications/roadmap-021313-v21.pdf.

4.2.2. SOHO/Last-Mile Issues

In order for DNSSEC to be useful, the results need to get to the devices that ask the questions, particularly to small-office/home office (SOHO) equipment. In many cases there have been broken software or hardware that make it difficult to get DNSSEC-validated answers though or, in the case of resolvers, to get answers that allow DNSSEC validation to take place.

To address these issues we have undertaken a number of efforts. In the prior contract we commissioned a testing effort and joined forces with Nominet to evaluate the state of home routers because these were considered possibly the weakest link in the DNSSEC chain. This work showed that a number of home routers prevented resolvers from doing DNSSEC validation when using the home routers' DNS resolvers, but in most cases resolvers bypassing the home router could perform DNSSEC validation. The results of this test have become standard for a number of ISPs when they evaluate new devices to give to customers.

Another source of network interference with validation is firewalls that have bad rules as to what DNS packets should look like; we have worked on getting these fixed.

As a part of the FCC Communications Security, Reliability, and Interoperability Council (CSRIC) effort (see Appendix A), we developed a suite of tests that allow us to classify resolver capabilities. These tests can be used to classify the behavior of ISP resolvers, and can help end customers check the state of the network they are attached to. We released a tool that runs these tests, DNSSEC Resolver Check (https://github.com/ogud/DNSSEC-resolver-check/), that is freely downloadable. We documented the results of our tests and are proposing to make them an industry standard via an Internet draft (http://tools.ietf.org/html/draft-ietf-dnsop-dnssec-roadblock-avoidance/).

These tests work well when dealing with two types of resolvers:

- Non-anycast resolvers
- Anycast resolvers where all the resolvers are equivalent

The tests report inaccurate answers when the anycast resolvers differ in behavior, which is frequently the case on "hotel" networks (i.e. networks that anyone can access, possibly after paying for access). These networks are in many cases set up to only allow limited use, rendering them quite hostile to any DNSSEC validation attempts. The DNSSEC-Trigger project that we have contributed to attempts to overcome this by using DNS over Transmission Control Protocol (TCP) or even DNS over Secure Sockets Layer (SSL). One of the important outcomes of our work is the realization that that a "mobile" host needs to perform a set of DNS tests before DNSSEC validation can take place or before users can expect dependable DNSSEC validation by upstream resolvers.

Deliverable:

- Roadblock avoidance (http://tools.ietf.org/wg/dnsop/draft-ietf-dnsop-dnssec-roadblock-avoidance/)

4.2.3. Timing Model

Deliverables:

- DNSSEC Timing Model Paper, February 2011
- Timing DNSSEC Changes, January 2011
- Internet Draft Memo Automating DNSSEC Delegation Trust Maintenance, June 2013 (http://tools.ietf.org/wg/dnsop/draft-ietf-dnsop-delegation-trust-maintainance/)
- Protocol for TLD and Reg Adoption, March 2011
- Transfer proposal, February 2014 (http://tools.ietf.org/html/draft-koch-dnsop-dnssec-operator-change/)

Another important issue is how DNSSEC is maintained when a domain is transferred from one DNS operator to another, and we participated in a number of task forces on DNSSEC transfers hosted by various European TLD operators. This issue is mainly relevant in the TLD case; thus, the solutions for this problem tend to be TLD-environment specific. The problem in a nutshell is that if a domain transfers to an operator that uses different keys to sign the zone, validators will treat the zone as bogus (i.e., validation fails) for a time. The goal of the work in this area was to create a description of a system that would allow the transfer to succeed without any validation errors. Out of this process came a proposal that uses the TLD operators' database as the conduit for keying information that the old DNS operator must insert into the zone before the transfer can start. The same logic applies when an enterprise changes DNS operators for one of its domains.

Once a domain is signed and the parent domain has a trust anchor for the domain as a DS record, whenever the child decides to change the trust anchor it needs to communicate with the parent the current set of trust anchors to advertise. This is a manual process, and we conducted studies on the timelines needed for these operations. One of our goals was to create DNS-protocol elements that could be automated at all levels of the DNS tree. Some work had gone into automating this in a special TLD case where the DNS operator is a registrar. Due to the fact the registrar has an API to the TLD, the operations can be performed over the API. In the general case, though, it is difficult for the DNS operator (the party managing the keys for the domain) to communicate with the parent, and this frequently occurs via a manual process. We have documented protocol extensions to the DNS that allow a child to publish in-zone its desire for the published trust anchor; the parent can then detect the records at the child and apply changes (if needed) to the trust anchor. A number of DNSSEC-provisioning tools have committed to implementing this standard once it is published (as of this writing, it is in the final stages of the IETF process; it has been approved and will be published as an official Request for Comment (RFC)).

The following is a more detailed discussion of the transfer process that resulted from the above work.

"Ripple-Free" Transfer of Signed Zones

Occasionally an owner of a zone may desire to change which organization is providing authoritative name service for the zone. *In principle*, the only thing that’s required is to copy the contents of the zone to the new operator and to put the names of the new operator’s name servers into the parent’s zone, i.e. change the name-server (NS) records in the parent zone. *In practice*, the transfer is more delicate. Depending on when the copying is done and when the change to the NS records in the parent is carried out, there might be a temporary disruption of service for the zone. Peculiarly, despite twenty-odd years of operation, documentation and practice of how to carry out such a transfer has never been solidified.

When DNSSEC is brought into the picture, the situation is more complicated and hence more delicate. Control of the private key that is used for signing is kept with the operator of the zone. Changing operators entails changing the private key. Hence, a change of operator includes a key rollover as well as a change in the set of name servers.

The question of how to transfer a signed zone from one operator to another was of specific concern during the approval process of the first major gTLD to support DNSSEC, .org, in order to prevent lock-in by a registrar. We investigated how to transfer a signed zone from one operator to another without losing service and without causing a break in the validation chains. We call this the "ripple-free" transfer of signed zones.

We developed scenarios for carrying out such transfers and tested them with two DNSSEC-capable registrars who also provided name service for their registrants, two other operators who provided name service but not registration service for customers, and one registry. In the course of developing these scenarios, we also provided scenarios for the basic operations of signing, unsigning and rolling over the keys in a signed zone, and for the transfer of unsigned zones.

Altogether we developed eight tests, grouped into three classes, and several of these tests had multiple variants. Table 2 below summarizes the tests. All of these tests were successful and were used as the basis for showing that multiple DNSSEC-capable registrars and DNS operators existed and that the transfer of an operational, signed zone from one to the other could succeed without any disruption of service or validation.

Table 2 – Transfer Cases for Signed Zones

The Following Tests Are Performed for Each Registrar

Test Grp	Test Class	Test	Registrars	Operators	Ext/Int	Description	Verification	Variants	# Current Registrar Role	# New Registrar Role
1	Basic Op	Signing	1	1	Either	Sign an unsigned zone	Verify it is signed and validates properly	Aa, Ac	2	
2	Basic Op	Unsigning	1	1	Either	Unsign a zone	Verify it is unsigned and operational	Aa, Ac	2	
3	Basic Op	Rollover	1	1	Either	Test rollover process w/o changing Regr or Opr	Show Rollover completes and validation is continuous	Aa, Ac	2	
4	Unsigned Xfr	Unsigned Opr Xfr	1	2	Ext	Regn Xfr, Unsigned Zone	Show all resolvers are able to fetch and validate w/o delay, outage or disruption	Ac->Ad	1	
5	Unsigned Xfr	Unsigned Opr & Regn Xfr	2	1	Int	Regr & Opr Xfr, Unsigned Zone	Show all resolvers are able to fetch and validate w/o delay, outage or disruption	Aa->Bb	1	1
6	Signed Xfr	Signed Regn Xfr	2	1	Ext	Regr Xfr, Signed Zone - No change of Opr	Show all resolvers are able to fetch and validate w/o delay, outage or disruption	Ac->Bc	1	1
7	Signed Xfr	Signed Opr Xfr	1	2	Ext plus either Int or Ext	Opr Xfr, Signed Zone - No change of Regr	Show all resolvers are able to fetch and validate w/o delay, outage or disruption	Ac->Ad Aa->Ac Ac->Aa	3	
8	Signed Xfr	Signed Zone Xfr btwn two Regr/Oprs	2	1	Int	Concurrent Change of both Regr and Opr for a Signed Zone	Show all resolvers are able to fetch and validate w/o delay, outage or disruption	Aa->Bb	1	1

4.2.4. Algorithm Signaling

Although most of the effort in the Deployment Initiative was focused on initial adoption and a variety of operational issues, we also looked at the long-term issue of facilitating changes in cryptographic algorithms. For example, advice from the expert crypto community regarding which hash algorithms to use has been changing relatively rapidly, e.g. Secure Hash Algorithm-1 (SHA-1) to SHA-256. It is believed that elliptic curve cryptography (ECC) algorithms will eventually replace the RSA algorithm.

The DNSSEC protocol supports the use of multiple algorithms. Each signature also carries a tag indicating which algorithms were used to create the signature. Thus, when a zone operator chooses to switch to a new algorithm, it can sign each record in its zone twice, once with the old algorithms and once with the new. Eventually, it can stop signing with the old algorithms and use only the new ones.

The zone operator can begin signing with both sets of algorithms whenever it wishes. Requesting systems that understand the new algorithms can check the signature using the new algorithms. Others will continue to rely on the signature created using the old algorithms.

When can the zone operator safely stop signing with the old algorithms? If it stops too soon, some of the requesters will not be able to validate the signature and may treat the zone as bogus and hence inaccessible. One possibility is to simply declare a "flag day," after which the old algorithms are not expected to be used. This may or may not work in practice. However, setting a flag day simply moves decisions about timing from individual zone operators to the overall community. In either case, it would help a lot to know whether the requesters are capable of using the new algorithms.

To facilitate the collection of that information, Scott Rose from the National Institute of Standards and Technology (NIST) and Steve Crocker from Shinkuro, Inc. designed an extension to the query side of the DNS protocol to include the set of algorithms understood on the requesting side. It is intended that this information, collected across a wide range of authoritative name servers and recursive resolvers, will provide reasonably accurate guidance on when new algorithms are implemented widely enough to permit full dependence on them, and hence permit a zone operator to stop signing with old algorithms.

At first glance it also appeared that including this information in a request might permit the responder to reduce an answer's size by choosing to include only one of the signatures in the event a record has been signed twice (or more). Unfortunately, because caching resolvers cannot know which algorithms will be understood by future requesters, caching resolvers must store the full set of signatures in a response from an authoritative name server, and, of course, authoritative name servers must deliver the full set of signed answers. Thus, the inclusion of information about which algorithms are understood by the requester cannot be used to trim the answers.

The extension of the DNS protocol to provide information about the algorithms known to the requester is now part of the official DNS protocol standard. It is defined in RFC 6975 (http://tools.ietf.org/html/rfc6975).

We are not aware that this extension has yet been included in any querying software, nor do we know of any effort to watch for this information in queries. These would be worthwhile efforts in the future.

4.2.5. History of TLD DNSSEC Adoption

In order to track both the history and planned future adoption of DNSSEC across the TLD community, we set up a database to record data about the various states of deployment. This database permits successive entries for the same piece of data, thereby tracking changes in estimated date of attainment.

We defined five benchmark dates that any TLD will encounter in the deployment process. These are:

> **Experimental:** The date when the TLD operator began or will begin initial technical experimentation with DNSSEC. This experimentation may or may not be visible on the Internet and may or may not be announced until well after it has begun.
>
> **Announcement:** The date when the TLD operator announced or plans to announce that it commits to signing its zone and accepting signed delegations sometime in the future. The announcement need not include when the signing will take place. The fact that a public commitment is being made is significant in its own right.
>
> **Partial:** The date when the public zone is first signed. This is called "partial" because it does not usually include the acceptance of DS records from child zones.
>
> **DS-in-Root:** After a zone is signed, a DS record is usually sent to the Internet Assigned Numbers Authority (IANA) to be included in the root zone. There may be a delay between the initial signing and the transmission of the DS record. Also, at the time this work was started, some TLDs were signed but the root zone was not yet signed and IANA was not accepting DS records.
>
> **Operational:** A zone is fully DNSSEC operational when it is signed and when it is accepting DS records from its registrants.

The database is organized to accept reports about each of these states for each TLD. Further, each entry includes a code for the degree of reliability based on the source of the information. In order of decreasing certainty, these are:

4. Observed through direct query over the Internet. This applies only to Partial and DS-in-Root and only for current status, not past or future
3. Reported by someone directly responsible for the TLD
2. Reported by someone knowledgeable about the TLD operation, e.g. a registry operator
1. All other reports

New reports are added to the database but old reports are not deleted unless they were wrong at the time they were added, e.g. an error in data entry. Queries to this database take into account that multiple records might exist for the same piece of data. For example, the first entry for the estimated date of full operation might be two years in the future. The next entry, say eight months later, might have a more reliable estimate. Entries for dates that have passed are generally more reliable than entries that give dates in the future.

This scheme provides a basis for recording what was expected and not only what actually happened. The maps at the beginning of this report are examples of reports created using data from this database.

After creating and operating the TLD-tracking process during the course of this contract, we have transferred responsibility for and control of this operation to the Internet Society with the agreement that they will continue to track and publish TLDs' DNSSEC information. A copy of our Memorandum of Understanding with the Internet Society, which lays out the details of this agreement, can be found in Appendix B: Memorandum of Understanding with the Internet Society below.

Our full, detailed description of the TLD data collection, collation and mapping processes is available at http://www.shinkuro.com/FA8750-10-C-0020/Publications/mapping-notes-v6-100113.pdf. The full set of information we delivered to the Internet Society is available at http://www.shinkuro.com/FA8750-10-C-0020/Publications/dnssecmap-138.src.tgz.

4.2.6. Tracking and Mapping DNSSEC Adoption

We have:

- Measured the number of TLD zones signed and their state
- Measured the use of DNS public key (DNSKEY) algorithms and NSEC/NSEC3 usage
- Attempted to quantify how prevalent validating was by looking at TLD query traffic
- Measured the number of open recursive resolvers and attempted to quantify them
- Monitored the behavior of validators relative to standards documents and classified them
- Measured whether the transfer of domains occurs without validation failure

We have conducted a number of measurement studies during this project to evaluate what the state of the DNS was during our project. These studies include measurements of whether TLDs are signed and the DNSSEC practices of TLD operators. This work is partially related to our DNSSEC map project as it allows us to monitor whether domains are in compliance with their plans, or when a TLD suddenly becomes signed. We did a number of studies on how to measure how widely used DNSSEC is, which included looking at traces of query traffic from a signed TLD operator. As part of our involvement with the FCC's CSRIC, we created a tool to classify how compliant a resolver is with DNS and DNSSEC specifications by sending the resolver a small number of queries.

Detecting DNSSEC validators among passive query traffic was difficult and unreliable. Open recursive resolvers are not considered a best practice on the Internet, but there are many of them and we conducted a scan of the whole Internet Protocol version 4 (IPv4) address space to count the number of "DNS responders," which included both resolvers and authoritative servers. In this experiment we used signed zones, which allowed us to detect a number of ISPs or other companies that perform DNSSEC validating. Finally, we attempted to classify the resolver using our classification tool.

We have developed techniques to perform statistical analysis of negative answers from signed domains to get estimates of the size of the domain as well as how the domain names are used. This work was motivated by the use of NSEC3 in many .gov domains for privacy reasons, which makes getting statistics from many of these domains difficult. Thus, we worked out statistical and brute force measurements techniques: All DNSSEC-signed domains can be walked, and for those that use NSEC, it is a simple task to just ask for the name right after the previous one to create a full chain, which would also tell us what kind of records reside at each name. At this point, we can classify the domain.

NSEC3-signed zones are little bit harder, but with simple random name generation, these can also be walked. We have developed tools that walk NSEC3-signed domain with only a minimal number of lookups. We have been working on creating a model that allows us to take a partial NSEC/NSEC3 chain and provide statistical estimates for the whole domain.

It turns out that due to NSEC3's properties it is much easer to create such models. We have used these techniques to see whether domains are signed down to lower levels or just at the top level. We can also be used to track whether a TLD is operational by counting the differences in DS records found over time. In the process of doing these checks, we discovered that it is not that difficult to reverse-map many domain names from NSEC3 records; all that's needed is a good graphics card and a good dictionary, as brute-force attacks are only effective on names containing less than 10 letters.

In addition to the above measurement studies, we believe there is value in having a coherent, comprehensive picture of the overall state of DNSSEC adoption by the world's TLDs. Such a picture would be the largest-scale reflection of various parties' progress in adopting DNSSEC in the past, present and future.

4.2.7. Users Guide

We worked with the Internet Society to create two deployment guides designed to introduce and demystify DNSSEC for decision-makers at ISPs and enterprises. These brief, two- or three-page guides were written at a level that would make clear to non-technical readers the benefits of DNSSEC while simultaneously giving them enough background to discuss DNSSEC signing with their technical staff, along with pointers to further resources. The ISP guide has been published on the Internet Society's Web site (http://www.internetsociety.org/deploy360/resources/deployment-guide-dnssec-for-isps/) while the enterprise guide was in production and awaiting publication at the time of this writing.

Deliverables:

- DNSSEC w/o Humans, June 2012 (http://www.shinkuro.com/FA8750-10-C-0020/Publications/DNSSEC w-o Humans-final.pptx)

5. CONCLUSIONS

This effort brings to a close approximately ten years of work supported by the U.S. Department of Homeland Security to foster the deployment of DNSSEC. There has been enormous progress during this period. Specifically:

- DNSSEC is now included in most of the DNS software, i.e. it is available to be used.
- The root is signed, thereby establishing a root key available for global use, and also signaling to the entire Internet community that DNSSEC is an integral part of the DNS infrastructure.
- All of the major top-level domains and a large number of the smaller ccTLDs are signed. ICANN has also required that all new TLDs created within its New gTLD Program must be signed from the beginning of their operation.
- Some major ISPs are checking (validating) DNSSEC signatures as part of the regular operation.
- Operational experience has been gained with keeping zones signed and transitioning a signed zone from one operator to another.
- Applications are being developed that rest on the DNSSEC infrastructure.

While these results are indeed important, full deployment and use of DNSSEC remains in the future. Only very few enterprises have signed their zones. The majority of ISPs have not chosen to validate DNS lookups. End systems are not yet asking for nor checking signed responses. There is more work to be done.

APPENDIX A: DNSSEC PRESENTATIONS AND TRANSCRIPTS

ICANN-related materials are available at:
http://public.icann.org/meetingarchives

ICANN Meeting, Nairobi, Kenya, March 2010

.ORG DNSSEC
DNSSEC Deployment Update
DNSSEC Deployment in Europe
AfTLD DNSSEC Survey
Open DNSSEC
Overview of Open Source Tools for DNSSEC
Rollover and Die?
DNS/DNSSEC and Domain Transfers: Are They Compatible?
DNSSEC for the Root Zone

FOSE 2010 Washington DC, March 2010

Materials available at:
https://www.dnssec-deployment.org/index.php/presentations-events-and-newsletters/dnssec-at-fose-2010/

What's next in DNSSEC: Overview
Advancing Federal DNSSEC Deployment: What to Look For in 2010
Deploying DNSSEC at the Root
Getting DNSSEC into Trusted Internet Connections
From Trust to Transparency: DNSSEC and Open Government
Government-funded Open Source Tools
Beyond Federal Deployment: The Next Wave
DNSSEC Implementation at ESnet
DNSSEC in US
Why DNSSEC Applies to More Federal Systems in 2010
Next Generation Risk Management
Updated Requirements from NIST Apply to More Federal Systems

Internet2 Meeting, Arlington, VA, April 2010

Transcript available at:
http://events.internet2.edu/2010/spring-mm/agenda.cfm?go=session&id=10001064&event=910

ICANN Meeting, Brussels, Belgium, June 2010

DNSSEC Workshop
DPS Framework: DNSSEC Policy and Practice Statement Framework
.ORG Transfer Tests Lessons Learned
DNS/DNSSEC and Domain Transfers: Are They Compatible?
Addressing DS Transfer: NSDS
DNSSEC.CZ

Deploying DNSSEC: Lessons Learned
Overview of Comcast's DNSSEC Work
DNSSEC Resolving at SURFnet
PowerDNSSEC: A Different Way of Doing Authoritative DNSSEC
Overview of Open Source Tools for DNSSEC
DNSSEC Progress in .UK
DNSSEC Implementation - Julien Adam
DNSSEC Rollout Status
The .DE DNSSEC Testbed
.EU DNSSEC Deployment
DNSSEC Deployment in .PT
Starting DNSSEC Deployment for .RU
Completing the Chain of Trust - Lance Wolak
Completing the DNSSEC Chain of Trust - Olaf Kolkman
Considerations in User Interface Design for DNSSEC
DNSSEC: Go Daddy Implementation
PIR – DNSSEC Chain of Trust
DNSSEC: A Foundation for Increasing Confidence in the Internet
DNSSEC for the Root Zone

Domain Name System Security DNSSEC Workshop Rome, Italy, July 2010
Materials available at:
http://www.gcsec.org/event/domain-name-system-security-dnssec-workshop

(Provided organizational help for this conference) (http://www.shinkuro.com/FA8750-10-C-0020/Publications/DNSSEC in the modern world.pdf)

ICANN Meeting, Cartagena, Uruguay, December 2010
DNSSEC.CZ
Preparing for and Rolling Out DNSSEC
Product Marketing - DNSSEC
Root Zone DNSSEC Deployment
.CO - Registry DNSSEC Plans
OpenDNSSEC
DNSSEC Implementation Approach Panel
Afilias - Deploying DNSSEC
LACTLD Update
Afilias Regional Update
DNSSEC Workshop
.SE Deployment Experience
DNSSEC at .BR Update
The DNSSEC Business Case (Or How to Create One)
Is There a Demand?
Tools for Deployment of DNSSEC
Premium DNS with DNSSEC GoDaddy.com
DNSSEC for Humans

DNSSEC Implementation Approaches
Nominet - Key Roll Issue
DNSSEC and the Practice Safe DNS campaign

ICANN Meeting, San Francisco, California, March 2011

Application Security with DNSSEC and DOSETA
VeriSign DNSSEC Update
DNSSEC Workshop
Mozilla
DNSSEC - Cisco
DNSSEC Deployment Plan
DNSSEC Validation Measurement
Innovative Uses As a Result of DNSSEC
VeriSign's DNSSEC Signing Service
DNSSEC Signing Service
Canadian Internet Registry Authority (CIRA)
DNSSEC Deployment Around the World
DNSX Secure Server
Fedora and DNSSEC
EURid DNSSEC Signing Services
Accelerating DNSSEC Signing
DNSSEC at Akamai Technologies
Innovative Uses As a Result of DNSSEC
Shared ccTLD DNSSEC Signing Platform
How IPv6 and DNSSEC Change the Intranets

OARC Workshop San Francisco, March 2011

Materials available at:
https://indico.dns-oarc.net//conferenceDisplay.py?confId=15

Conclusions from DNSSEC Traces (http://www.shinkuro.com/FA8750-10-C-0020/Publications/Improving DNS contents in the RRR world-final.pdf and http://www.shinkuro.com/FA8750-10-C-0020/Publications/Improving DNS contents in the RRR world-final.pptx)

IETF 80, Prague, Czech Republic, March–April 2011

DNS for Programmers (http://www.ietf.org/edu/documents/80DNS-Koch-Gudmundsson.pdf)

Securing and Trusting Internet Names (SATIN), Teddington, UK, April 2011

Materials available at:
http://conferences.npl.co.uk/satin/agenda2011.html

Motivations and Terminology for DNSSEC Operations Handover (http://www.shinkuro.com/FA8750-10-C-0020/Publications/satin2011-Crocker.pdf)

ICANN Meeting, Singapore, Singapore, June 2011

DNSSEC Workshop - Singapore - Program Slides
DNSSEC in the Glue... A Operational Tale
DNSSEC Deployment in .JP
Number of DNSSEC Validators Seen at JP
DNSSEC for DE: Developing the Testbed into Production Service
DNSSEC Challenges for Registrars
DNSSEC Deployment Around the World
.th DNSSEC Updates
Panel: Signed Domain Transfer
.my DNSSEC Deployment Plans & Experience
Key Deletion Issues and Other DNSSEC Stories
Introducing DNSSEC Into .nz
DNSSEC Research at SURFnet
Verisign DNSSEC Deployment Update
DNSSEC: Registrar Challenges

FOSE 2011 Washington DC, July 2011

Materials available at:
https://www.dnssec-deployment.org/index.php/presentations-events-and-newsletters/dnssec-at-fose-2011/

DNSSEC in US Federal Systems
DNS-2 Where does DNSSEC Deployment stand in .gov? A status update
OMB and FISMA require DNSSEC deployment. How does your agency's deployment stack up against other federal sites? A status report on what .gov has accomplished and what remains to be done.
The Gov Domain
Where does DNSSEC stand in .Gov
The State of DNSSEC in .Gov
DNS-3: Private Sector Deployment in .com, .net, .org and Beyond
Lessons government IT managers can learn from other sectors and countries' deployment of DNSSEC.
VeriSign DNSSEC Deployment Update
DNSSEC Deployment in .UK
.ORG Moving Forward
DNS-4: The Drive to Validation: Real-life Lessons
The Drive to Validation
DNSSEC and FISMA Update
DNS-5: What to Ask Vendors about DNSSEC
DNS-6: Beyond Infrastructure: Emerging DNSSEC Apps and APIs
DNSSEC Applications: Troubleshooting Tools

ICANN Meeting, Dakar, Senegal, October 2011

Challenges and Benefits of DNSSEC for Africa
Afnic - DNSSEC Updates

FCC CSRIC III - Working Group 5 - DNSSEC Implementation Practices
DNSSEC Deployment Update
AfTLD Update
UK Top Level Domain Update
Panel Discussion: Challenges and Benefits of DNSSEC for Africa and Regional Update
DNSSEC at AFRINIC
DNSSEC .CZ
DNSSEC Deployment Around the World
.NA’s First Experiences With the PCH Signing Platform
DNSSEC Workshop - Dakar - Program Slides
A Look At TLD DNSSEC Related Queries
PROTECT-IP (COICA)
DNSSEC In Operation
NIC .sn
The Mensa project - Measuring DNS Health and Security
How IPv6 and DNSSEC change the Intranets
DNSSEC Update for DE
Internet Society Perspectives on Domain Name System (DNS) Filtering
Internet Engineers' Letter Urging Amendment of the PROTECT-IP Act
Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill

Global IPv6 Summit, Taipei, Taiwan, November 2011

TWCERT/CC Information Security Series: The Global Trend of DNSSEC (http://www.shinkuro.com/FA8750-10-C-0020/Publications/DNSSEC in the modern world.pdf)

ICANN Meeting, San Jose, Costa Rica, March 2012

ICANN DNSSEC Workshop - Comcast's Operational Experiences
Looking at TLD DNSSEC Practices
PayPal DNSSEC Experience
Using DNSSEC to Protect Reputations El Caso del Banco Nacional
DNSSEC Signer Implementation Hardware
DNSSEC at .br update
DNS Sec Para el Banco Nacional
.CO DNSSEC - Status, Challenges & Benefits
National Bank
DNSSEC in .SE
MyDNSSEC - DNSSEC for the end user
DNSSEC Workshop - Costa Rica - Program Slides
DNSSEC Update on ".kr" & Supporting activity for domestic stakeholder
DNSSEC Deployment Around the World
Challenges and Opportunities in DNSSEC Deployment and Usage

FOSE 2012 Washington DC, April 2012
Materials available at:
https://www.dnssec-deployment.org/index.php/presentations-events-and-newsletters/dnssec-at-fose-2012/

Update on .gov
The uptake of DNSSEC in the .gov zone
VeriSign on the services they offer to and through .gov
FISMA, with emphasis on mobile requirements
Applications and Dane
Report on NLnet Labs DNSSEC Trigger
Chrome and Mozilla DNSSEC plug-ins Developed by .cz
Reengineering Trust: Towards The Domain Key Infrastructure
National Strategy for Trusted Identity in Cyberspace

ICANN Regional Meeting, Prague, Czech Republic, June 2012
DNSSEC Workshop
DNSSEC & PowerDNS Large Scale DNSSEC Deployments
DENIC's First Year in DNSSEC
DNSSEC @ .PL - Selection of HSM Solution
The Great DNSSEC Quiz
DNSSEC Visualization for the End-User
DNSSEC Deployment Around the World
DNSSEC Deployment by a Registrar
.EU DNSSEC Deployment
DNSSEC in .RU
DNSSEC in .SE
DNSSEC.CZ
AFNIC Community DNSSEC Adoption
DNSSEC in UA - Status Update
DNSSEC Activities @ NIC.AT
2 Years of DNSSEC @ ccTLD .PT
DNSSEC Trigger
DNSSEC w/o Humans?
DNSSEC - Tools for DNSSEC Automation and Management
Evolution of DNSSEC in BIND9
CreDNS
DANE – A Killer App for DNSSEC?

ICANN Meeting, Toronto, Canada October 2012
DNSSEC Workshop: Canadian Internet Registration Authority (CIRA)
Update on .GOV
DNSSEC.CZ
Solutions to Help People Implement DNSSEC
Encouraging DNSSEC Adoption: What Has Worked and What Hasn’t
Secure Zones During Transfers

Registry Failover and DNSSEC
Encouraging DNSSEC Adoption, What Has Worked and What Hasn't the .br experience
DNSSEC Deployment Around the World
DNSSEC .GOV Uptake
OS Integrating of DNSSEC
DNSSEC and the New gTLD Program
Next Steps In Accelerating DNSSEC Deployment
DNSSEC Workshop
DNSSEC Activities In North America: Comcast
DNSSEC at Vidéotron
AFNIC DNSSEC Adoption
DNSSEC @ Neustar
.nl DNSSEC Deployment
DNSSEC Portfolio Checker
Encouraging DNSSEC Adaptation
DNSSEC and Fragmentation: A Prickly Combination
Migrating a High-value Domain While Maintaining Inner Peace
Presentation: DNSSEC in the RRR World (http://www.shinkuro.com/FA8750-10-C-0020/Publications/Improving DNS contents in the RRR world-final.pptx)

FCC Working Group 5, CSRIC III, February 2013
Materials available at:
http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG5_Report_March_%202013.pdf

DNSSEC Implementation Practices for ISPs, Final Report on Measurement of DNSSEC Deployment

ICANN Meeting, Beijing, PRC, April 2013
DNSSEC Workshop
Use of DNSSEC in the Reverse Name Space
Parallel ZSK/KSK Rollover Scheme
How to Use DNSSEC to Keep PKI on a Leash
DANE and Innovation
Introduction to the DANE Protocol
Bloodhound: DNSSEC and DANE for the End-User
Influence of DNSSEC
CNNIC DNSSEC Deployment in the Region
Operational Aspects of Root Zone KSK Rollover
DNSSEC Key Rollover in the Root Zone
Survey of Recursive Resolvers
EPP keyrelay: A Solution for DNS Operator Changes with DNSSEC
DNSSEC Disaster Recovery
The Operational Realities of DNSSEC
DNSSEC: Regulative, Legislative and Persuasive Approaches to Encouraging Deployment

DNSSEC Activities in Asia Pacific
DNSSEC Deployment Around the World
DNSSEC Adoption at the Top
CENTR Domain Counter
SANNET DNSSEC Experience
Community Activities in Japan
The DNSSEC Debate in .uk
DNSSEC at ARIN
DNSSEC on the Reverse Tree
A DNSSEC Operational Gap
DNSSEC in the Reverse Tree @ LACNIC
DNSSEC - How Can I Help
DNSSEC in .nz

OARC Meeting Dublin, May 2013
Materials available at:
https://indico.dns-oarc.net//contributionListDisplay.py?confId=0

Classifying Resolver Capabilities (http://www.shinkuro.com/FA8750-10-C-0020/Publications/Classifying resolvers.pdf)

ICANN Meeting, Durban, South Africa, July 2013
DNSSEC Activities in Africa | ICANN DNSSEC Roadshow
Introduction to the DANE Protocol
DNSSEC for Managers - The Three Spheres
DNSSEC Deployment Around the World | Counts, Counts, Counts
GoDaddy DNSSEC
DNSSEC Workshop | Update on Root Key Rollover
DNSSEC Workshop
DNSSEC - How Can I Help?
DNSSEC Obligations in the RAA
Is the World Upside Down?
DANE and SMTP: TLS Protection for SMTP | Using DANE and DNSSEC
Key Management in JP
RU-CENTER DNSSEC Experience and Expectations (Registrar Point of View)
Technical Parameter Decisions for DNSSEC
DNSSEC Ready Registry System
DNSSEC MoU
DNSSEC Activities in Africa | ISPs, Registries, and Registrars

ICANN Meeting, Buenos Aires, Argentina, November 2013
DNSSEC Workshop
2013 RAA & DNSSEC
DNSSEC and Registrars?
DNSSEC Automated Tools
Root Zone KSK

DS TTL Shortening Experience in .JP
DNSSEC in the Reverse Tree @LACNIC
Introduction to the DANE Protocol and Updates from IETF 88
NIC Argentina
Guidance for Registrars in Supporting
DNSSEC Deployment in Enterprises: A Multi-stakeholder Game
Survey on the Structure of DNSSEC Workshops
DNSSEC Experience at NIC Chile (...so far)
SAC063: SSAC Advisory on DNSSEC Key Rollover in the Root Zone
A Threshold Cryptographic Backend for DNSSEC
DNSSEC Activities in Latin America
Deploying DNSSEC in the .CA Registry
.CO DNSSEC | Experiences and Challenges
DNSSEC - How Can I Help?
DNSSEC for the Enterprise: Why, When & How
DNSSEC in (Medium/Small) ccTLD Registries
Automating Maintenance of Delegation Information
Negative Trust Anchors

ICANN Meeting, Singapore, March 2014

DANE Demonstration
DNSSEC Workshop
CDS, CDNSKEY
DNSSEC Workshop
Deployment of DNSSEC at .ee
DNSSEC Apps
DNSSEC Deployment in .cn
DNSSEC - How Can I Help?
DNSSEC: IP Mirror
DNSSEC Obligations in the 2013 Registrar Accreditation Agreement (RAA)
DNNSEC Research and Experimentation Status in Vietnam
Measuring DNS Use
.nz DNSSEC
SAC063: SSAC Advisory on DNSSEC Key Rollover in the Root Zone
DNSSEC Validation Monitor
The Last Millimetre

LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS

AES	Advanced Encryption Standard
API	Application Programming Interface
ccTLD	Country-Code Top-Level Domain
CDN	Content Delivery Network
CIO	Chief Information Officer
CSRIC	Communications Security, Reliability, and Interoperability Council
DANE	DNS-based Authentication of Named Entities
DES	Data Encryption Standard
DHS	Department of Homeland Security
DKIM	Domain Keys Identified Mail
DNS	Domain Name System
DNS-OARC	DNS Operations Analysis and Research Center
DNSKEY	DNS public Key
DNSSEC	Domain Name System Security Extensions
DPS	DNSSEC Practice Statement
DS	Delegation Signer
ECC	Elliptic Curve Cryptography
FCC	Federal Communications Commission
gTLD	Generic Top Level Domains
HSM	Hardware Security Module
ICANN	Internet Corporation for Assigned Names and Numbers
IDN	Internationalized Domain Name
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
ISP	Internet Service Provider
IT	Information Technology
KSK	Key-Signing Key
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NS	Name Server
NSEC	Next Secure (data format)
NSEC3	Next Secure 3 (data format)
OS	Operating System
PKI	Public-Key Infrastructure
RFC	Request for Comment
RSA	Encryption standard developed by RSA, Inc.
SHA	Secure Hash Algorithm
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SOHO	Small-Office/Home Office
SPF	Sender Policy Framework
SSL	Secure Sockets Layer

TAR	Trust Anchor Repository
TCP	Transmission Control Protocol
TLD	Top-Level Domain
TLS	Transport-Layer Security
TTL	Time to Live
UDP	User Datagram Protocol